Remarks

Objection to the Drawings

In the Office Action the drawings were objected to, since Figure 4 was referred to in the Specification and was not received by the Office in the Drawings file and/or copy.

In reply, Applicant submits herewith a new sheet containing Figure 4. Applicant respectfully submits that the addition of Figure 4 does not introduce new matter for at least two reasons. First, Figure 4 is found in the same form as Figure 3 in the priority application (US Provisional Application No. 60/534,190). The only difference is a change in reference numerals. Second, Figure 4 is supported by the text of the as-filed application. Accordingly, Applicant respectfully requests entry of Figure 4.

Amendments to the Specification

A cross reference to the U.S. provisional priority application has been added. No new matter has been added.

35 U.S.C. §101 Rejections

In the Office Action, claims 1-10 were rejected under 35 U.S.C. § 101, as for having non-statutory subject matter.

The Applicant has replaced claim 1 with a newly drafted claim 21, inter alia, to overcome the Office Action rejection under 35 U.S.C. § 101.

Therefore, the Applicant respectfully requests the Examiner to withdraw the rejections under 35 U.S.C. § 101.

35 U.S.C. §102 Rejections

In the Office Action, claims 1-20 were rejected under 35 U.S.C. 102 (e) as being anticipated by Carter ET al. (U.S. 2003/0051026).

The Applicant has drafted and presents newly drafted independent Claims 22 and 23 in this Response to distinctly point out the subject matter of the invention.

The Applicant's Invention:

Newly added Claim 21 teaches a system for real time monitoring and controlling of sessions within a network server environment. Each original session enables operating a sequence of processes including operations carried out in the server environment (e.g. one or more servers configured in, for example, single or multi tier architecture) enabling to communicate and operate processes arriving from multiple client users using various portals (e.g. network pages activities) by operating various communication sessions.

The system includes one or more computerized modules installed in the server environment, where the module(s) enable associating a session ID to each original session of each client user and to each process in the sequence of processes operated by the original session. The session ID enables determining an authorization level according to predefined determination rules, relating to the manner in which the client user has operated the original session (e.g. the way the user has entered the network page and the manner in which the communication was executed, etc.).

Each process in the sequence is also associated, in real time, with the same session ID of the original session the process is related to (since each session operates a sequences of associated processes), enabling the module to continuously monitor operation of each process of each client user. Each process is carried out by the server environment, according to the authorization level related to the session ID of the process, associated thereto in real time (e.g. enabling or disabling the process, which next process in the sequence to execute and the like).

Similarly, newly added Claim 22 teaches a method for real time monitoring and controlling of communication sessions within a network server environment. Each original session enables operating a sequence of processes including operations carried out in the server environment (e.g. one or more servers configured in, for example, single or multi tier architecture) enabling to communicate and operate processes arriving from multiple client users using various portals (e.g. network pages activities) by operating various communication sessions.

The method enables associating a session ID to each original session and to each process in the sequence of processes operated by the original session. The session ID enables determining an authorization level according to predefined determination rules, relating to the manner in which the client user has operated the original session.

Each process in the sequence is also associated, in real time, with the same session ID of the original session that the process is related to (since each session operates a sequences of associated processes) and therefore an authorization level is defined to each process in real time, thereby enabling to continuously monitor operation of each process of each client user. The process's operation (e.g. enabling or disabling the process) is carried out according to the authorization level related to the session ID of the process.

Carter

Carter teaches "a system that monitors and protects the security of computer networks uses artificial intelligence, including learning algorithms, neural networks and genetic programming, to learn from security events. The invention maintains a knowledge base of security events that updates autonomously in real time. The invention encrypts communications to exchange changes in its knowledge base with separate security systems protecting other computer networks. The invention autonomously alters its security policies in response to ongoing events. The invention tracks network communication traffic from inception at a well-known port throughout the duration of the communication including monitoring of any port the communication is switched to. The invention is able to track and utilize UNIX processes for monitoring, threat detection, and threat response functions. The invention is able to subdivide the network communications into identifying tags for tracking and control of the communications without incurring lags in response times."(Carter, Abstract).

According to Carter, "**The User Identification Matrix is also used to associate a given user ID with a given process ID running on the system at any given time. Once a User Identification Matrix is completed, a user ID can be selected from the User Identification Matrix to find all the processes associated with each user and compiled within a single column within the Process Control Matrix.**" (Carter, paragraph [0342]).

"The Permissions Control Matrix is generated by taking information from the User Control Vector and constructing a two column Matrix using the user's permissions for the directory being accessed by the user, and another column for the permissions of the file the user is accessing…The tracking and subsequent monitoring of communications from users is conducted with TCP Port control vectors, a TCP Port Control Matrix, and a TCP Port-Definitions Control Matrix at the Communication Infrastructure and Interface Layer and the Expert System Security Intelligence Layer." (Carter, paragraphs [0348-0349]).

"The comparison of the User/Group Permissions Matrix and the Permissions Control Matrix are made with an adaptation of matrix multiplication. The elements of each matrix are matched to each other as in matrix multiplication in their above order, but the matched elements are then evaluated for correspondence, rather than multiplied." (Carter, paragraph [0363])

Carter enables individually associating a user ID to each process ran by the system to enable later tracking of the association of the processes (meaning which process is associated with which user). Carter does not associate an ID that relates to the original communication session (e.g. whether the entrance to a webpage has been carried out through entering security codes or was it a free entry webpage). Carter's system is an AI system which enables automotive learning of the users' behavior by tracking processes carried out while identifying the user from which the processes originated. This allows Carter to learn the behavior of the user while carrying out communications and update authorization knowledge bases (see Carter, Abstract quoted above).

Conversely, the Applicant provides a system that allows associating IDs by identifying the session and therefore its related authorization (rather than the user's identification) and associating the session ID to each process operated due to the execution of the original session to allow real time operating the processes relating to the session according to the session ID's related authorization.

Each session, according to the Applicant, is related to an authorization level and the session authorization level may depend on the communication link or the portal configuration (e.g. whether the web page is a free entry page or whether it requires inserting entrance codes) as well as the manner in which the user has utilized the specific configuration of the portal or link to execute the communication session.

Carter does not teach a method or a system that allows associating identifiers to processes according to the processes' original communication session, which defines authorization level of the session and thereby of each process associated with the original session.

Since Carter's object is to acquire knowledge relating to the user, Carter does not operate the processes according to the authorization level of each process, deduced from the authorization level of the original session the process is associated with.

Therefore, the Applicants respectfully request that the Examiner withdraw the rejection under 35 U.S.C. 102 (e) in light of the above clarifications and in light of the newly revised independent claims 21 and 22.

Claims 2-10 and 12-20 depend directly or indirectly on independent claims 21 and 22, which replace the former independent claims 1 and 11 to receive status of allowance.

Therefore, the rejection of claims 2-10 and 12-20 is assumed to have been overcome.

Conclusion

In view of the foregoing amendments, revision and remarks, the pending claims are deemed to be allowable. Their favorable reconsideration and allowance is respectfully requested.

Should the Examiner have any question or comment as to the form, content or entry of this Response and Amendment, the Examiner is requested to contact the undersigned at the telephone number below. Similarly, if there are any further issues yet to be resolved to advance the prosecution of this application to issue, the Examiner is requested to telephone the undersigned counsel.

Fees for a two month extension of time are believed to be due for this submission and are being paid via credit card. However, please charge any required fee (or credit overpayments) to the Deposit Account of the undersigned, Account No. 500601(Docket No. 7044-X06-007).

Respectfully submitted,

/Paul D. Bianco/

Paul D. Bianco, Reg. # 43,500

Customer Number: 27317
FLEIT GIBBONS GUTMAN BONGINI & BIANCO P.L.
21355 East Dixie Highway, Suite 115
Miami, Florida 33180
Tel: 305-830-2600; Fax: 305-830-2605
e-mail: pbianco@fggbb.com